



Link to this free resource
You can add a hyperlink to our Network security Glossary using one of the code snippets below.

```
<!-- start of Sec-1 link code -->  
<a  
href="http://www.se  
c-  
1.com/glossary/">Ne  
twork Security  
Glossary</a>
```

[ABOUT US](#) [SOLUTIONS](#) [TESTIMONIALS](#) [RESOURCES](#) [CONTACT US](#)

[Home](#) > [Network Security Glossary](#) > **D**

Network Security Resources Sec-1 Network Security Glossary

D

Daemon

A program that runs continuously and exists for the purpose of handling periodic service requests that a computer system expects to receive. The daemon program forwards the requests to other programs (or processes) as appropriate. Each server of pages on the Web has an HTTPD or Hypertext Transfer Protocol daemon that continually waits for requests to come in from Web clients and their users.

Data driven attack

A form of intrusion in which the attack is encoded in seemingly innocuous data, and it is subsequently executed by a user or other software to actually implement the attack.

DES (Data Encryption Standard)

A widely-used method of data encryption using a private (secret) key that was judged so difficult to break by the U.S. government that it was restricted for exportation to other countries. There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used. For each given message, the key is chosen at random from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key.

Denial of service attack

A user or program takes up all the system resources by launching a multitude of requests, leaving no resources and thereby "denying" service to other users. Typically, denial-of-service attacks are aimed at bandwidth control.

DHCP (Dynamic Host Configuration Protocol)

DHCP enables individual computers on an IP network to extract their configurations from a server (the 'DHCP server') or servers. In particular, servers that have no exact information about the individual computers until they request the information. The overall purpose of this is to reduce the work necessary to administer a large IP network. The most significant piece of information distributed in this manner is the IP address.

Diffie-Hellman

The Diffie-Hellman Method For Key Agreement allows two hosts to create and share a secret key. VPNs operating on the IPSec standard use the Diffie-Hellman method for key management. Key management in IPSec begins with the overall framework called the Internet Security Association and Key Management Protocol (ISAKMP). Within that framework is the Internet Key Exchange (IKE) protocol. IKE relies on yet another protocol known as OAKLEY and it uses Diffie-Hellman.

DiffServ (Differentiated Services).

Differential service mechanisms allow providers to allocate different levels of service to different users of the Internet. Broadly speaking, any traffic management or bandwidth control mechanism that treats different users

differently - ranging from simple Weighted Fair Queuing to RSVP and per-session traffic scheduling - counts. However, in common Internet usage the term is coming to mean any relatively simple, lightweight mechanism that does not depend entirely on per-flow resource reservation.

Digital Certificate

A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting and decrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

Digital Signature

A digital signature is an electronic rather than a written signature that can be used by someone to authenticate the identity of the sender of a message or of the signer of a document. It can also be used to ensure that the original content of the message or document that has been conveyed is unchanged. Additional benefits to the use of a digital signature are that it is easily transportable, cannot be easily repudiated, cannot be imitated by someone else, and can be automatically time-stamped.

DMZ (de-militarized zone)

A network added between a protected network and an external network in order to provide an additional layer of security. Sometimes called a perimeter network.

DNS (Domain Name System)

The Internet protocol for mapping host names, domain names and aliases to IP addresses.

DNS spoofing

Breaching the trust relationship by assuming the DNS name of another system. This is usually accomplished by either corrupting the name service cache of a victim system or by compromising a domain name server for a valid domain.

Domain

The unique name used to identify an Internet network.

Domain name server

A repository of addressing information for specific Internet hosts. Name servers use the domain name system to map IP addresses to Internet hosts.

Downloadable

A "downloadable" is a file that has been transmitted from one computer system to another, usually smaller computer system. From the Internet user's point-of-view, to download a file is to request it from another computer (or from a Web page on another computer) and to receive it.

Downstream post office

A post office that communicates with a mail server through another post office or other post offices.

DSL (Digital Subscriber Line)

DSL (Digital Subscriber Line) is a technology for bringing high-bandwidth information to homes and small businesses over ordinary copper telephone lines. xDSL refers to different variations of DSL, such as ADSL, HDSL, and RADSL. A DSL line can carry both data and voice signals and the data part of the line is continuously connected.

DSS (Digital Signature Standard)

The Digital Signature Standard (DSS) is a cryptographic standard promulgated by the National Institute of Standards and Technology (NIST) in 1994. It has been

BEST AVAILABLE COPY

adopted as the federal standard for authenticating electronic documents, much as a written signature verifies the authenticity of a paper document.

DSX (Dynamic Security Extension)

A proprietary technology that is patented and works in the following way. The operating system has a system call (or vector) table that contains memory address pointers for each system call. These pointers point to a location in memory where the actual kernel code of the system calls resides. DSX stores the address pointers for the security sensitive system calls and then redirects these pointers to the corresponding SECURED system call code, which is located elsewhere in memory.

Dual-homed gateway

A system that has two or more network interfaces, each of which is connected to a different network. In firewall configurations, a dual-homed gateway usually acts to block or filter some or all of the traffic trying to pass between the networks.

[^ Back to top](#)

[« Back to Glossary index](#)

[Contact us](#) | [Site map](#)

Copyright © 2003 Sec-1 Limited

[UP TO TOP](#)

BEST AVAILABLE COPY



Link to this free resource
You can add a hyperlink to our Network security Glossary using one of the code snippets below.

```
<!-- start of Sec-1 link code -->  
<a  
href="http://www.se  
c-  
1.com/glossary/">Ne  
twork Security  
Glossary</a>
```

ABOUT US

SOLUTIONS

TESTIMONIALS

RESOURCES

CONTACT US

Home > Network Security Glossary > C

Network Security Resources Sec-1 Network Security Glossary

C

CA (Certificate Authority)
See Certificate Authority

CA Signature

A digital code that vouches for the authenticity of a digital certificate. The CA signature is provided by the certificate authority (CA) that issued the certificate.

CGI exploit

When a denial of service attack is aimed at the CGI (common gateway interface), it is referred to as a CGI exploit. The CGI is a standard way for a Web server to pass a Web user's request to an application program and to receive data back to forward to the user. It is part of the Web's HTTP protocol.

Certificate Authority (CA)

A certificate authority is an authority in a network that issues and manages security credentials and public keys for message encryption and decryption. As part of a public key infrastructure (PKI), a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate.

Challenge-Response

A common authentication technique whereby an individual is prompted (the challenge) to provide some private information (the response). Most security systems that rely on smart cards are based on challenge-response. A user is given a code (the challenge) which he or she enters into the smart card. The smart card then displays a new code (the response) that the user can present to log in.

CHAP (Challenge-Handshake Authentication Protocol)

An authentication technique where after a link is established, a server sends a challenge to the requestor. The requestor responds with a value obtained by using a one-way hash function. The server checks the response by comparing it to its own calculation of the expected hash value. If the values match, the authentication is acknowledged otherwise the connection is usually terminated.

Checksum or hash

A checksum is a count of the number of bits in a transmission unit that is included with the unit so that the receiver can check to see whether the same number of bits arrived. If the counts match, it's assumed that the complete transmission was received.

Circuit-level gateways

Circuit-level gateways run proxy applications at the session layer instead of the application layer. They can't distinguish different applications that run on the same protocol stack. However, these gateways don't need a new module for every new application, either. Circuit-level gateway is a firewall feature which can, when needed, serve as an alternative to packet filtering or application

BEST AVAILABLE COPY

gateway functionality.

Cleanup interval

A setting in the Ravlin Node Manager that specifies how long a Ravlin unit waits before performing automatic internal cleanup. In general, the busier the network, the more often system cleanups should be performed.

Client

A client is the requesting program or user in a client/server relationship. For example, the user of a Web browser is effectively making client requests for pages from servers all over the Web. The browser itself is a client in its relationship with the computer that is getting and returning the requested HTML file.

Community string

A character string used to identify valid sources for SNMP requests, and to limit the scope of accessible information. Ravlin units use the community string like a password, allowing only a limited set of management stations to access its MIB.

Content blocking

The ability to block network traffic based on actual packet content.

Content filtering, scanning or screening

The ability to review the actual information that an end user sees when using a specific Internet application. For example, the content of e-mail.

Content virus

See data driven attack. Commonly protected against with a virus scanner.

Cookie

A message given to a Web browser by a Web server. The browser stores the message in a text file called cookie.txt. The message is then sent back to the server each time the browser requests a page from the server.

CoS (Class of Service)

Class of Service (CoS) is a way of managing traffic in a network by grouping similar types of traffic (for example, e-mail, streaming video, voice, large document file transfer) together and treating each type as a class with its own level of service priority.

CryptoCore®

A RedCreek hardware implementation that offloads the heavy computational load usually imposed by cryptographic tasks, freeing system resources and thus allowing rapid encryption.

Cryptography

A branch of complex mathematics and engineering devoted to protecting information from unwanted access. In the context of computer networking, cryptography consists of encryption, authentication, and authorization.

[^ Back to top](#)

[« Back to Glossary Index](#)

[Contact us](#) | [Site map](#)

Copyright © 2003 Sec-1 Limited

[Back to top](#)

BEST AVAILABLE COPY